Rule Statement

It is the responsibility of the information resource owner or designee to ensure that adequate security measures are in place and that an annual risk assessment is performed.

Definitions

**Confidential Information** - Information that is excluded from disclosure requirements under the provisions of the Texas Public Information Act or other applicable state or federal laws.

**Mission Critical Information** - Information that is defined by the System Offices (SO) or information resource owner to be essential to the continued performance of the mission of the SO or resource owner mission. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, and failure to comply with regulations or legal obligations, or closure of the department.

**Information Resource Owner** – an entity responsible for:
- a business function; and,
- determining controls and access to information resources supporting that business function.

**Custodian** - A person (or department) providing operational support for an information system and having responsibility for implementing owner-defined controls and access privileges.

**Information Resources (IR)** - The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

**ISAAC (Information Security Awareness Assessment and Compliance)** - A web-based system used to assess the security posture of information systems and measure compliance with the Information Security Standards. It also provides guides for creating a disaster recovery plan and performing a physical security check.
1. GENERAL

1.1 The SO electronic information resources are vital administrative assets which require appropriate safeguards. Computer systems, networks, and data are vulnerable to a variety of threats. These threats have the potential to compromise the integrity, availability, and confidentiality of the information.

1.2 Effective security management programs must be employed to appropriately eliminate or mitigate the risks posed by potential threats to the SO information resources. Measures shall be taken to protect these resources against unauthorized access, disclosure, modification or destruction whether accidental or deliberate.

1.3 The SO, as an institution of higher education, is required to comply with the Texas Administrative Code (TAC) “Information Security Standards”. The TAC assigns responsibility for protection of informational resources to the Chancellor. For the purposes of this rule, the authority and responsibility regarding the System Offices’ compliance with the TAC Information Security Standards has been delegated to the System Chief Information Officer (SCIO).

2. RESPONSIBILITIES

2.1 The SCIO has designated the responsibility for administering the provisions of this rule and the TAC Information Security Standards to the System Offices Information Security Officer.

2.2 The director of a department shall be responsible for ensuring that an appropriate security program is in effect and that compliance with this rule and TAC Information Security Standards is maintained for information systems owned and operationally supported by the department.

2.3 The director of a department which provides operational support (custodian) for information systems owned by another SO department, or System member shall have the responsibility for ensuring that an appropriate security program is in effect and that compliance with TAC Information Security Standards is maintained for the supported information systems.

2.4 Operational responsibility for compliance with TAC Information Security Standards may be delegated to the appropriate information system support personnel (e.g. System Administrators) within the department.

2.5 The information resource owner, or their designee, is responsible for ensuring that the risk mitigation measures described in applicable System Offices Rules and Standard Administrative Procedures (SAP) are implemented. Based on risk
management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures. All exclusions must be in accordance with SAP 29.01.99.S1.27 Exclusions from Required Risk Mitigation Measures.

2.6 Mission Critical or Confidential Information maintained on information resources such as servers, individual workstations, and portable devices must be afforded the appropriate safeguards stated in the TAC Information Security Standards and applicable System Offices Rules and Standard Administrative Procedures. It is the responsibility of the information resource owner or designee to ensure that adequate security measures are in place and that an annual risk assessment is performed.

3. COMPLIANCE ASSESSMENT REPORTING

3.1 Departments having ownership or custodial responsibility for electronic information systems shall ensure that on an annual basis, a security assessment report is filed with the SCIO. This report is produced by the Information Security Awareness Assessment and Compliance (ISAAC) system.

3.2 Departments having responsibility for information resources which store, transmit, or process mission critical or confidential information may assess their security posture and measure their compliance with the TAC Information Security Standards by using the ISAAC system.

Related Statutes, Policies, or Requirements

1 Texas Administrative Code (TAC) Chapter 202 as amended or supplemented

Contact Office

Office of the Texas A&M University System Chief Information Officer